Microsoft Exchange Server

Chapter 6.2
Implementing Administration and Maintenance Procedures

Planning Guide

Abstract

This chapter outlines planning considerations for Exchange 2000 performance monitoring. After completing these steps, planners and messaging operations personnel should be able to both proactively and reactively monitor Exchange 2000 performance to confirm system health, diagnose common system performance problems, plan for growth and optimize performance. This chapter contains high-level material that is relevant to your Senior IT Decision Maker, IT Manager, Senior Systems Architect/Programmer, Support Analyst, Implementer, and Support Specialist (Helpdesk).

However this chapter is primarily targeted at the IT Manager who is responsible for creating an appropriate support organization to manage deployed Exchange 2000 Messaging and Collaboration Services, and the Support Analysts and Specialists who are responsible for day-to-day operations, support and maintenance.

This is a preview edition of the Microsoft Exchange 2000 Server Upgrade Series. The final documentation will be available in November 2000.

© 2000 Microsoft Corporation. All rights reserved.

THIS IS PRELIMINARY DOCUMENTATION. The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Microsoft, Active Directory, Windows, Windows NT and the Windows logo are registered trademarks of Microsoft Corporation.

Other product or company names mentioned herein may be the trademarks of their respective owners.

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

1000

CONTENTS

INTRODUCTION.....1
Goals 2

PROCESS FLOWCHARTS.....3
Maintenance 3
Design Considerations 8
Active Directory 8
Third Party Tools 10
Changes from Exchange 5.5 12
What to Monitor 13
How to Monitor 18
Event Viewer 18
Resource Requirements 32
Teaming 32
Security and Account Privileges 33
Escalation Model (example) 34
First Tier – Process 35
Second Tier – Solution 35
Third Tier – Crises Management 36
IT Management 36

MONITORING EXCHANGE SERVER AVAILABILITY.....37

SUMMARY.....38
Links 38

INTRODUCTION

Management and monitoring of your Exchange organization should be considered an integral part of your initial design effort. This chapter will help you prepare your organization to monitor and maintain your Exchange 2000 infrastructure according to the needs you defined in Chapter 2, and your defined service levels.

This chapter presumes that you are running Exchange 2000 in mixed-mode, which can accommodate all versions of Exchange Server. By default, Exchange 2000 is installed in mixed mode.

To other Microsoft Exchange Server 4.0, 5.0, and 5.5 computers in the site, the Exchange 2000 Server computer appears as just another server, and on the whole is monitored using the same procedures. The servers send out directory replication notifications as usual, and the Site Replication Service (SRS) database requests changes the same way that earlier versions of Exchange Server request changes.

Mixed mode exists to maintain backward compatibility, but mixed mode limits the system to the constraints that are imposed by earlier software releases. In a mixed mode site, the rules that apply to earlier versions of Exchange Server apply to Exchange 2000 as well; for example, all servers in the site must use a common service account.

The following limitations apply to Exchange 2000 when Exchange 2000 is running in mixed mode:

- Exchange Server 5.0 and 5.5 sites are mapped directly to administrative groups.
- Administrative groups are mapped directly to Exchange Server 5.0 and 5.5 sites.
- Servers cannot be moved between administrative groups.
- Routing group membership consists only of servers that are installed in the administrative groups.

You can change an Exchange 2000 organization to native mode after all of the servers are upgraded to Exchange 2000 and earlier release restrictions no longer apply. You cannot switch to native mode until you either upgrade or decommission all earlier versions of Exchange Server.

The following are some of the features of Exchange 2000 native mode:

- Support for multiple routing groups.
- Routing groups can consist of servers from multiple administrative groups.
- Ability to move servers between routing groups.

- Simple Mail Transfer Protocol (SMTP) is the default routing protocol.

Goals

To focus your performance measurement process, you must first define your service level metrics. In other words, you should first monitor those things that have a direct effect on your agreed service levels throughout both deployment and daily operation. This is important for three reasons:

- **Problem Notification:** Monitoring tools can alert you to problems early so that they can be addressed as quickly as possible, perhaps before any user impact.
- **Troubleshooting:** When a problem arises, management and monitoring tools allow you to identify and isolate the problem for quick corrective action.
- **Capacity Planning:** Metrics about your system in normal operation are valuable for predicting how the system scales to meet your needs.

Identifying and eliminating a design-related problem in the planning and design phase is much cheaper and easier than after implementation, and puts you in a much better position to make any unanticipated adjustments you discover as a result of your pilot testing. Thoughtful planning, as well as well-defined, scalable enterprise messaging goals and consistent and proactive system management and monitoring reduces downtime, speeds troubleshooting and allows your organization to realize the best return on your Exchange investment.

At minimum you should define:

- Service Delivery Parameters
  - System availability
  - Average message delivery time (organization-wide)
  - Maximum backup and restore time
- Service Usage Assumptions
  - Maximum user mailbox size
  - Average message size
  - Average number of active users
  - Average number of messages sent per user per day

You have dual planning and operational goals: efficiency (administer and monitoring correctly), and effectiveness (administer and monitor the right things). The goal of this chapter is to assist you in successfully planning your Exchange 2000 administration and maintenance process and

PROCESS FLOWCHARTS

systems. Best practices and lessons learned in administrating and maintaining Exchange 2000 are shared as a reference. What to measure, how, how often, and what actions to take based on the results, will be detailed in template form or with specific examples to illustrate.

You should also consider using Microsoft's large network of Microsoft Certified Solution Providers and Consulting Services to help you configure and prepare your operations environment, troubleshooting procedures, and recovery plans.

Focus on people and processes as much as on technology when planning for maintenance of your Exchange organization. In addition, your network and Windows 2000 infrastructure are key elements to understanding your Exchange organization's condition at any given moment.

Before you begin your maintenance planning you should have already prepared your:

- Operational staffing plan, including:
  - Exchange System Administration
  - Windows 2000 System Administration
  - Monitoring
  - Directory Services administration
  - Security administration
- Staff training plan
- Backup and recovery plan
- Troubleshooting plan
- Change control enforcement plan
- Disaster Recovery plan and
  - Prepared your standby server and recovery kit

Maintenance

Follow a three-step process to prepare your monitoring and management plan:

1. Prepare for service monitoring and management
2. Perform service monitoring
3. Perform incident management

The process flowcharts on the following pages (Figures 1-3) illustrate the high-level service monitoring and management processes.

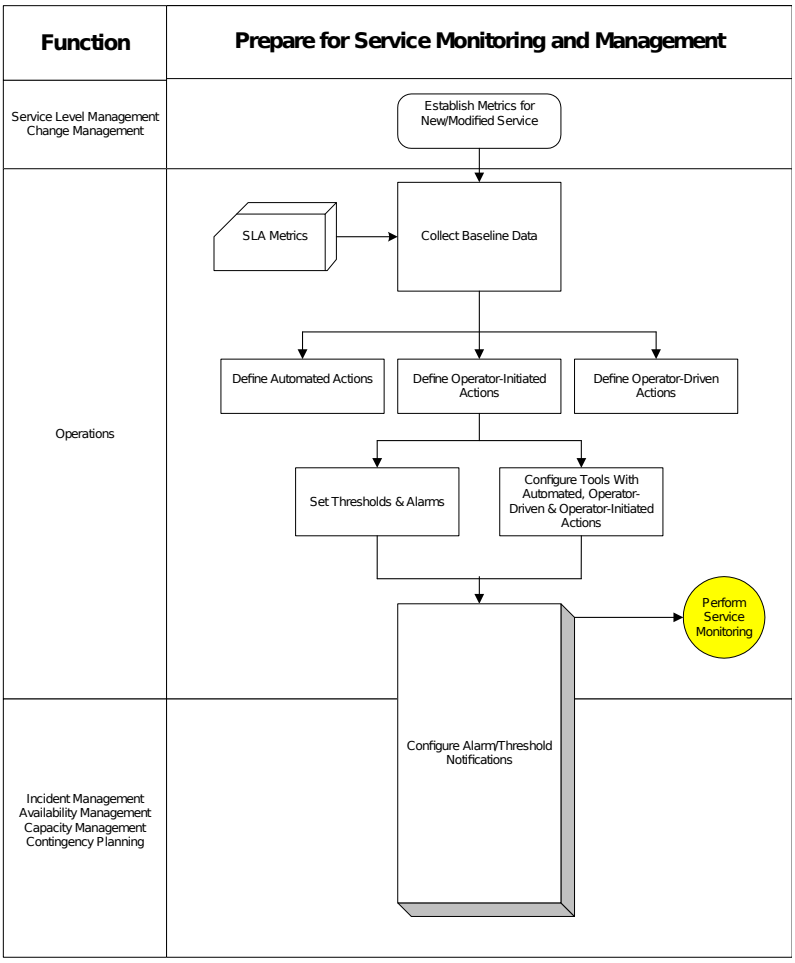


Figure 1 Prepare for Service Monitoring & Control Process

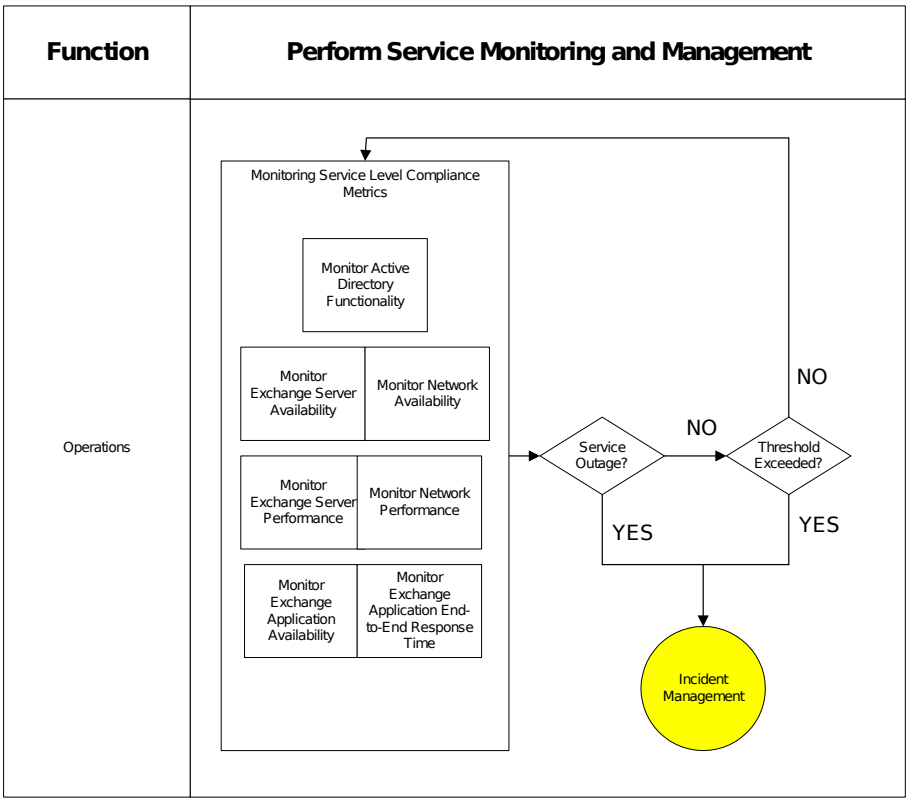


Figure 2 Perform Service Monitoring Process

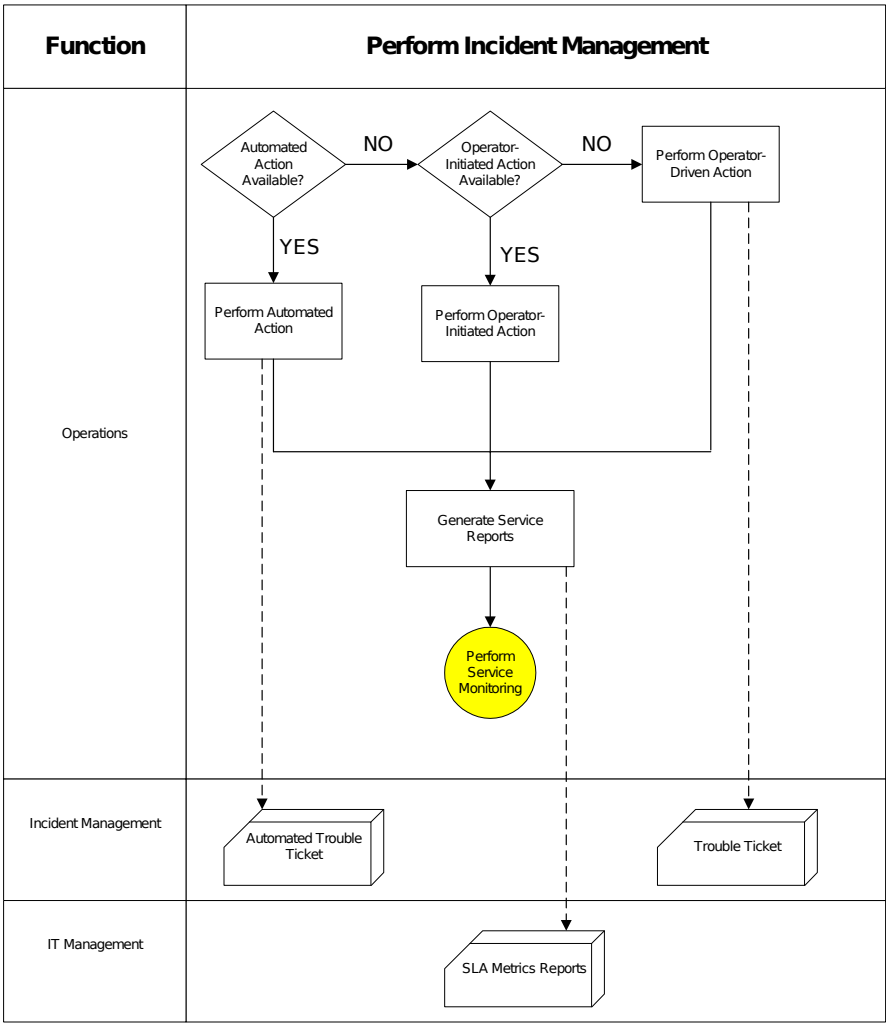


Figure 3 Perform Service Control Process

The Service Level Agreement SLA metrics reports should include:

Availability Report	Periodic report (usually monthly), generated from the event logs of your Exchange 2000 servers showing uptime and down-time for the period
Event Report	Periodic report (usually daily) generated from the event logs (and trouble ticket system, if used), detailing critical events and the actions taken to resolve them
Performance Report	Periodic report showing average and periodic work queue lengths, disk space usage, messaging statistics and delivery times

Throughout this chapter, the roles and processes in the Microsoft

Operations Framework (MOF) are used for illustration. In your organization, one person or department may perform more than one of the roles and functions shown. The MOF model is a simplified but realistic model that is highly effective for both large organizations with teams fulfilling the roles, as well as for small organizations that may have one person in several combined roles. The key to effective implementation is consistent and regular monitoring of the metrics defined in your service level agreements, combined with consistent incident management and change control.

The MOF maps five major service delivery functions, each of which has different roles in managing and maintaining your Exchange 2000 organization:

The Service Level Management function is responsible for:

- identifying, negotiating, monitoring and reviewing Service Level Agreements (SLA)
  - the terms of the SLA will determine the baseline objects operations must monitor in order to determine compliance; for example, your SLA may specify “99.5% availability and e-mail message delivery anywhere in the world in 5 minutes”

The Availability Management function is responsible for:

- reliability, resilience, maintainability and serviceability
- calculating availability
- planning, monitoring and reporting
  - your daily operational monitoring procedures will be your first alert and starting point for troubleshooting availability issues
  - historical logging will allow you to analyze and report long-term availability

The Capacity Management function is responsible for:

- performance, workload, resource and demand management
- application sizing and modeling
  - to predict your future capacity needs, you will need daily usage monitoring information. For example, if you designed your storage groups with a 25% overhead for growth, you need to know when and how often your storage groups exceed 75% of the allocated disk space
  - You can use a stress tool such as the Exchange Stress and Performance (ESP) tool in the Exchange 2000 Resource Kit to progressively load your server’s hardware until it fails to meet required demand, note the maximum level of activity your server can handle, and set your monitoring and alerting threshold to a percentage of that maximum. The ESP tool has several modules,

allowing you to test multiple protocols such as Http-DAV, IMAP4, LDAP, NNTP, OLEDB, POP3, and SMTP.
  - As your storage groups grow, so will the amount of time you need to back them up. At some point, you will need to add capacity in order to maintain the service level metric you have established for backup (for example, backing up all storage groups in less than one hour).

The Contingency Planning function is responsible for:

- risk analysis and management
- assets, threats and vulnerabilities
- countermeasures
- development, testing and maintenance of the contingency plan
  - Performance monitoring is important for detecting out-of-bounds activity which may indicate attack

The Cost Management function is responsible for:

- costing and charging
  - Just defining and agreeing on service level metrics spotlights the link between costs, usage and service level provision
- capital costs and running costs
- charging policy
  - Daily use monitoring over time is important for establishing the cost per user or resource cost
  - The Message Tracking Center in Exchange 2000 can be used for detailed metrics if you are interested in a charge-by-use model

The MOF divides operations into four phases, as illustrated in Figure 4 below:

1. Changing
2. Operating
3. Supporting
4. Optimizing

IT Service Management Functions (SMFs) are the core of the MOF process model. Although no SMF is exclusive to a given phase in MOF, each has a home phase, or primary planning and execution phase. Grouping them with a primary MOF phase is a more intuitive way to introduce an SMF in the context of the process model. The following diagram depicts the grouping of SMFs and their primary phase within the process model. For more information on MOF, SMFs, and the process model of operations, see the white paper at: http://www.microsoft.com/TechNet/maintain/mofovrv.asp.

Design Considerations

Active Directory

Windows 2000 Active Directory is a primary design requirement for Exchange 2000. Exchange 2000 uses Active Directory as its directory store. It is critical that you quickly and clearly differentiate Active Directory (Domain Controller/Global Catalog) performance issues from Exchange performance during daily operations, and understand the potential Exchange performance impacts from changes to Active Directory.

In addition, you should work out clear responsibilities for Active Directory services and object management. You might have had two separate teams in your Exchange 5.5 organization: one for Exchange directory services, and one for Windows NT directory services. Since Exchange 2000 does not have its own directory service, you have the opportunity to consolidate ownership into one team.

For example, installing Exchange 2000 and setting up your Active Directory Connectors (ADCs) require extension of the Active Directory schema. Your line-of-business application development efforts might also require extending the schema. Since schema extensions are irreversible, you will want to plan and control this process carefully. You need to clearly identify ownership and responsibilities for Active Directory.

In the example LMO two directory service environment, different IT groups had separate and clear roles/responsibilities. For example, the Exchange 5.5 Operations group owned the creation and management of mailbox objects. The Windows Accounts group owned creation and management of user objects. As the Exchange directory and Active Directory services merged these two objects into one, it became clear that someone needed to be responsible for the management of these objects, and, by extension, management of the Active Directory schema that holds them. This overlap of required knowledge exposed the need for a new role in the organization—temporarily called Schema Architect/Schema Administrator (SAA).

The SAA’s role is a hybrid. It includes some of the responsibilities formerly held by Exchange administrators, and other responsibilities once under Windows administrator control. It also assumes new responsibilities related to the new integrated directory environment including:

- Development of a schema tracking database and monitoring/management tools to identify who extends the schema, why, and with what information. This allows future groups to locate schema extensions and determine if the information they wish to access (for a new workflow or line of business application, for example) already exists in Active Directory.

- Management of schema extensions, for any reason. The SAA evaluates schema extensions against base schema and proposed extensions so that future schema extensions are made safely and do not overlap existing or planned extensions.
- Installing the ADC and configuring Connection Agreements. For example, the account used to install the ADC must have full administrative permissions to Active Directory (including permissions to modify the schema), as well as Exchange 5.5 and Exchange 2000 full administrator and Account Operator permissions. The example LMO's pre-Exchange 2000 administrative model separated messaging and Windows 2000 administrator permissions. Exchange administrators had full permissions to Exchange, but not Active Directory. Windows administrators had user account permissions, but no permissions on mailboxes.
- Management of schema content, which helps when deciding the impact of adding directory object attributes to Global Catalog (GC) replication, because excessive indexing of GC attributes potentially degrades query performance.

The SAA role is indicative of the new level of interoperation and interdependence between the IT groups managing Windows and Exchange. For example, SAA Exchange 5.5 server roles and permissions are summarized in Table 1.

Exchange 5.5 Right	Service Account Admin	Permission Admin	Admin	View-Only Admin	User	SAA
Add Child	Yes	Yes	Yes	No	No	Yes
Modify User Attributes	Yes	Yes	Yes	No	Yes	Yes
Modify Admin Attributes	Yes	Yes	Yes	No	No	Yes
Delete	Yes	Yes	Yes	No	No	Yes
Send As	Yes	No	No	No	Yes	Yes
Mailbox Owner	Yes	No	No	No	Yes	Yes
Logon Rights	Yes	Yes	Yes	No	Yes	Yes
Replication	Yes	No	No	No	No	Yes

Modify Permissions	Yes	Yes	No	No	No	Yes
Search	No	No	No	No	No	Yes

You need the security and administration models you developed in the first part of Chapter 6 to assign monitoring duties to the appropriate groups with the minimum level permissions needed to do daily monitoring, and advanced troubleshooting beyond that.

Third Party Tools

Microsoft Exchange Server 2000 provides both reactive and proactive system management tools. The proactive tools can continuously search for potential problems, and you can program them to take automatic corrective actions. The Windows 2000 and the Exchange 2000 Resource Kits provide additional useful tools. You can combine these tools to produce a complete monitoring solution. However, if you are an LMO organization, you will want to combine those functions and automate your data collection, analysis and alerting tasks across tens or hundreds of servers in a single unified management and monitoring system.

A number of third party enterprise tools are available, including Microsoft SMS, NetIQ, SeNTry, CA FastLane, NetPro, Unicenter, Tivoli, and others, each with their own strengths and weaknesses. Each has differences in their ability to integrate any other monitoring systems you may have or want to put in place, and different built-in reporting capabilities. The procedures and tasks discussed in this chapter apply to one system, or to hundreds under the automation of a third party tool.

You can also use Windows Management Interface (WMI) scripting and Windows Scripting Host (WSH) to design specialized solutions to meet your specific needs through many different interfaces, such as CDO, ADO, LDAP, and ADSI. WMI ships with built-in providers (or standard providers) including:

- **Active Directory Provider**, which acts as a gateway to all the information stored in the Active Directory service. You can access both WMI and Active Directory information using a single API.
- **Performance Counter Provider**, which exposes the raw performance counter information used to compute the performance values shown in the System Monitor tool. Any performance counters installed on a system will automatically be visible through this provider.
- **Registry Provider,** which allows Registry keys to be created, read, and written. WMI events can be generated when specified Registry

keys are modified.

- **SNMP Provider,** which acts as a gateway to your OEM systems and devices that use the Simple Network Management Protocol (SNMP) for management. SNMP Management Information Base (MIB) object variables can be read and written. You can automatically map SNMP traps to WMI events.
- **Event Log Provider,** which provides access to data and event notifications from the Windows 2000 Event Log.
- **Win32 Provider,** which provides information about the operating system, computer system, peripheral devices, file systems, and security information.
- **WDM Provider,** which supplies low level Windows Driver Model driver information for user input devices, storage devices, network interfaces, and communications ports.
- **View Provider**, which allows new aggregated classes to be built up from existing classes. Source classes can be filtered for only the information you want, information from multiple classes can be combined into a single class, and data from multiple machines can be aggregated into a single view.

WMI also provides support for third party custom providers You can use these to service requests related to managed objects that are environment-specific, using the WMI API to access the Common Information Model (CIM) Object Manager repository and to respond to CIM Object Manager requests made by applications.

The Exchange 2000 Resource Kit also includes a Web-based monitoring tool that gives you snapshot health metrics across your Exchange organization. For more information on the Web Monitor Tool, see the Exchange 2000 Resource Kit.

The example LMO , for instance, combines several third party tools and custom WMI scripted solutions into one centralized console view of all their Exchange 2000 servers worldwide. Figure 5 illustrates a high-level view of this consolidation.

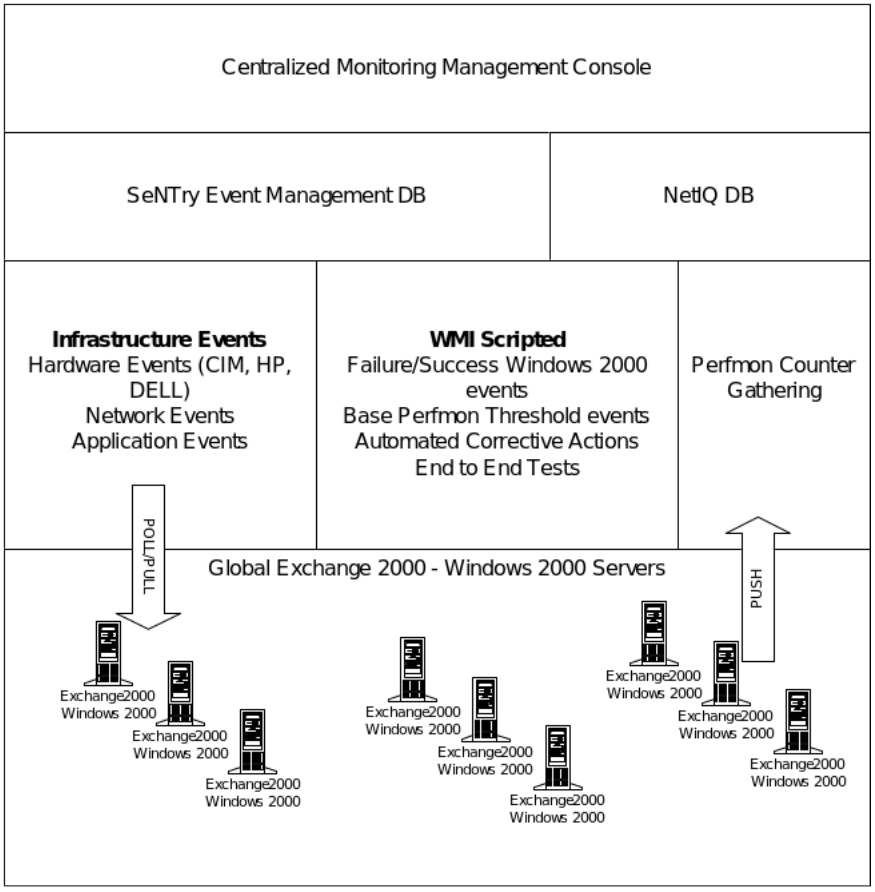


Figure 4 Server consolidation

For detailed information on using Windows Scripting Host and WMI to design your own solutions, see http://www.microsoft.com/windows2000/library/howitworks/management/wmiscripts.asp, and “Building Management Components for Microsoft Exchange 2000 Server” at http://msdn.microsoft.com/library/techart/e2k_cmpts.htm.

Changes from Exchange 5.5

Although most of your monitoring and managing tools and procedures from Exchange 5.5 for core messaging services will continue to work, there are new roles and responsibilities (such as responsibility for schema extensions to Active Directory), as well as new things to consider now that Exchange no longer has its own directory.

During the coexistence period, while you still have Exchange 5.5 servers in your environment, you will need to continue your Exchange 5.5 performance monitoring procedures.

For example, you may have tuned your Exchange 5.5 server performance using the Microsoft Exchange Server Performance Optimizer (PerfWiz). Based on your choices, files written by the various Exchange components

(Information Store, MTA, etc.) could be assigned to specific fixed disks depending upon available storage.

Exchange Server 2000 does not use a Performance Optimizer-like tool because it is capable of dynamically changing certain parameters as needed for optimum performance. You will need to manually configure and optimize beyond these built-in dynamic changes.

When you upgrade your Exchange 5.5 servers to Exchange 2000, some registry keys altered by PerfWiz retain their PerfWiz values, some do not, and some keys no longer appear in the registry or appear in a different location. You should start over in setting up your monitoring and optimizing plans when you upgrade, because of the significant improvements made to Exchange 2000, and because your Exchange 5.5 optimizations do not necessarily carry over and might not be appropriate any longer.

Document your Exchange 5.5 settings before upgrading to Exchange 2000. Copy the *WINNT\System32\perfopt.log* text file to preserve a record of those registry keys and disk assignments changed by PerfWiz.

The design specifications, hardware configuration, and specific role of the Exchange server you designed in Chapter 2 must be taken into account when configuring and monitoring each system. For example, you will define different disk space thresholds for a mailbox server with 3,000 mailboxes than for a mailbox server with 100 or 1,000 mailboxes. In the same way, the disk space thresholds to monitor for a hub server are different than those for a mailbox server or public folder server.

The remainder of this chapter discusses performance monitoring procedures and counters that are common among Exchange 2000 servers roles, except where noted.

What to Monitor

All problem identification in your Exchange environment will be fundamentally based on the information in the event log and performance monitor counters.

Monitoring is the act of determining compliance to agreed-upon service levels—not determining why they are not being met. Although important, error detection, incident management and problem resolution are more tactically focused activities than monitoring for compliance, and are covered in more detail in the white paper at http://www.microsoft.com/TechNet/win2000/operatio.asp

Windows 2000 performance monitoring can be broken into four main resources to monitor:

- Processor
- Memory

- Disk I/O
- Network I/O

Processor

The System Monitor counter to examine the processor activity is **Processor\% Processor Time**. You should proactively monitor so that this counter is not consistently near 100%. You can also use the Task Manager CPU Usage History section Performance property sheet for an instant snapshot of performance.

To determine the specific process that is utilizing processor cycles:

1. Select the **% Processor Time** instance of the **Process** object in System Monitor
2. Click the second instance (below "_Total"), and drag the mouse down to include every instance.
3. Either scroll up and **Ctrl+click** to remove the **Idle** instance, or delete it later.
4. Click **Add**.

This will show every process on the system by percentage of processor utilization. To make the chart easier to read:

1. Right-click **Performance Display** and click **Properties**.
2. Change the **View** section from **Graph** to **Histogram**.
3. Click **OK**.
4. Press **Ctrl+H** to enable highlighting.

You can now scroll through the histogram of all the active processes on the system with the up and down arrows, and the instance that is in focus will be highlighted. This will allow you to determine the process using the most processor time.

Key Processor Counters

Object	Counter	Scale	Instance
Processor	% Processor Time	1.0	0 (1, 2, etc for muti-processor)
Process	% Processor Time	1.0	Each process running on the system will have an instance

Memory

The System Monitor counter to examine the system memory usage is **Memory\Available Bytes**. This counter should be as high as possible and always over at least 4 MB. You can also use the **Task Manager**

Performance property sheet, **Physical Memory** section, **Available counter** to quickly view memory usage.

As an indicator of the amount of free memory in the system, when this value drops below 4MB, the system paging rate increases in an attempt to free up memory. A decrease in available bytes over time indicates a memory leak condition. To determine the culprit, monitor the **Private Bytes** counter of the **Process** object, and watch for a process with a steadily increasing **Private Bytes** value.

Monitor the **Paging File\% Usage** and **Paging File\% Usage Peak** counters for values near 100%. Allowing the page file to grow can significantly impact system performance. As a best practice, use a "doorstop" file (2-3 GB) on each logical disk with a pre-determined filename to prevent running out of free drive space. If you are alerted to a hard-drive full error, you can quickly delete the doorstop file to enable quick recovery while you make further diagnoses or corrective action. The **Process\Page File Bytes** counter can be used to determine which process is using the most page file space on the system.

In addition to monitoring the page file usage, you should monitor how much paging is occurring in the system by watching the **Memory\ Pages/sec** and **Memory\Page Faults/sec** counters for heavy usage.

Key Memory Counters

Object	Counter	Scale	Instance
Memory	Available Bytes	0.000001	N/A
Paging File	% Usage	1.0	_Total and one for every paging file.
Paging File	% Usage Peak	1.0	_Total and one for every paging file.
Process	Page File Bytes	0.000001.	Each process running on the system will have an instance
Process	Private Bytes	0.00001	Each process running on the system will have an instance

Disk I/O

To monitor disk I/O, monitor the following System Monitor counters:

- **Physical Disk\% Disk Time**. This is the percentage of time that this disk drive is busy servicing read or write requests. This counter should be as low as possible, and if it is consistently at or near 67%, this indicates a disk bottleneck.

- **Physical Disk\ Avg. Disk Queue Length**. Any time the queue length on an I/O device is greater than 1 or 2, it indicates significant congestion for the device.

Key Disk Counters

Object	Counter	Scale	Instance
Physical Disk	% Disk Time	1.0	_Total and one for every physical disk attached to the system.
Physical Disk	Avg. Disk Queue Length	100.0	_Total and one for every physical disk attached to the system.

Network I/O

To monitor your network I/O, monitor the **Network Interface\Bytes Total/sec** counter to determine the throughput of your server's network card.

Object	Counter	Scale	Instance
Network Interface	Bytes Total/Sec	0.0001	One for each network adapter installed in the system

Note that in a large, distributed IT environment, collecting and analyzing large volumes of data from remote systems can incur significant system and human overhead (disk storage, CPU cycles to process large volume of data, and others). Over-aggressive monitoring can in itself *cause* performance issues. An alternative approach is to instrument and collect just the right metric for meeting your agreed-upon service levels. Use the same tools, moved up to higher logging levels, to troubleshoot most problems. This also has performance impacts, so plan your monitoring operations and processes to handle the routine high-level monitoring of daily operations. In that way, you can concentrate efforts on troubleshooting problems quickly and effectively when they arise.

Finally, independent studies (Gartner 1998), as well as Microsoft's internal experiences, show that the major causes of downtime (across operating systems) are:

- Application Failure – roughly 40%, resulting from
  - Poor testing
  - Poor change management
  - Overloaded
  - Poor problem detection
- Operator Error – roughly 40%, resulting from
  - Forgetting something

  - Poor procedures
  - Backup errors/security
- Other – roughly 20%
  - Hardware/OS failures
  - Network failures
  - Power failure/Disaster

Since the majority of these are not related to monitoring at all, you can have the greatest impact on your system uptime by first concentrating your efforts on the people and process areas, such as thorough testing, change control, and reducing operator errors.

The key to monitoring and managing the remaining items (hardware, operating system, network, and application), is to accept and design for the reality that at any given time these systems will exhibit a performance bottleneck. One subsystem will always have more load than another. A bottleneck occurs when a task on the system must wait for a system resource (processor, memory, disk, or network) because it is tied up with another task. Bottlenecks equal degraded performance.

You will frequently find that one bottleneck masks another. A heavily loaded system can have several bottlenecks, but until the first bottleneck is corrected, it might be the only one showing. For example, a system with inadequate CPU resources may show processor use at 100%, but the disk I/O at manageable levels. Upgrading the processor or adding a second processor removes that bottleneck, allowing the system to make I/O requests unhindered by a slow processor—but then you might find that the disk I/O becomes the bottleneck.

You can reduce your monitoring and management burden and increase your effectiveness by collecting metrics from three basic sets:

Health Monitoring. A small number of metrics (1-10) giving you a daily high-level view of system, subsystem, or application health and service level compliance. Use these metrics in a real-time or near real-time context in a management-by-exception model. Management-by-exception notification to a centralized Web reporting page can significantly reduce your network overhead. You can adapt and customize the Web Monitoring Tool in the Exchange 2000 Resource Kit for this purpose.

You can setup the Web Monitoring Tool to show you the crucial health indicators for all your Exchange servers:

- Server’s CPU status
- Server’s memory status
- Server’s logical disk status
- Server’s SMTP, X.400 and connector queue status

High-to-Medium Level Problem Resolution Metric. For incident management (problem detection, identification and resolution) triggered by the alerts you configure, a larger number of metrics (say, up to 40) are needed to drill down into the problem. The idea is to collect and present enough metrics to understand the problem or non-compliance situation roughly 80% of the time, but not to overburden the human operator or agent program with excessive detail. In many cases, you will log these metrics over a set period of time to give a clear picture of the issue.

You should also archive these metrics to support your capacity planning.

In both cases, log data locally and keep it for a short period of time (up to 30 days), then archive to another media or a central repository for long-term data storage and centralized management and reporting.

Detailed Troubleshooting, Optimization or Capacity Planning Metrics. This set requires as many metrics as necessary to solve the other 20% of the problems or for capacity planning. You can incur significant performance degradation collecting this information, so you

will want to keep the collection period as short as necessary to give you the information you need. For example, if you use Performance Monitor (Perfmon) to monitor a server remotely, you increase network I/O as the performance data is sent over the network to the computer running Perfmon. Again, you will want to keep the duration as short as is needed to diagnose the problem, and then move this information to a central repository for centralized reporting and capacity planning.

These three sets of metrics are reflected in most events you view in the event logs:

- events with **Informational** severity indicate that the event is useful for trend analysis purposes, but a response is not required
- events with **Warning** severity indicate a low-priority problem
- events with **Error** severity indicate that a response in real time is required

Monitoring your Exchange organization for service level compliance is your first step. In normal day-to-day operations, providing that your operational environment is well-understood and infrastructure is properly designed, problems are the exception, not the rule.

How to Monitor

Event Viewer

Microsoft Exchange Server logs all of its error messages and warnings in the Windows 2000 application event log, as do other applications. Windows 2000 also logs messages about its own operations in the system application log. These errors can be viewed and filtered through the Event Viewer MMC snap-in. A central log of this sort makes diagnosis of problems much easier—especially when all of the system errors go in the same place; for example, those specific to Microsoft Exchange Server as well as networking, device driver, security, and other types of problems/warnings.

Exchange Server logs critical events to the Windows 2000 application log. Each Exchange component can be configured to generate high levels of logging should the need arise. In the normal course of events, these logging levels should all be set to their minimum level, "none", to avoid filling the event logs too rapidly and placing an unnecessary burden on your systems and consuming your free hard disk space.

The Windows 2000 Resource Kit includes utilities that can dump the contents of event logs to files for subsequent analysis. There are also third party tools that have sophisticated event log processing facilities and are able to look for situations, such as a log entry for backup starting but no event logged for backup completion.

You should scan the event logs of Exchange servers every few days at a

minimum.

Service Stop Application Log Events

Each service logs an event to the Application Log when a stop has completed.

Service	Event Source	Event Number
Internet Mail Connector (5.5)	MSExchangeIMC	1001
Messaging Transfer Agent (5.5)	MSExchangeMTA	9299
Information Store (5.5 and 2000)	MSExchangeIS Public	1006
	MSExchangeIS Private	1006
Directory (5.5)	MSExchangeDS	1003
System Attendant (5.5 and 2000)	MSExchangeSA	1003

The following table lists and describes the possible message events in Exchange 2000 and the corresponding topological representations. Some of these (from Exchange 5.5) will no longer be of interest when you achieve your Exchange 2000 native-mode environment. All new Exchange 2000 events are in the range 1019 to 1031.

Event #	Event Type	Description
0	Message transfer in	The MTA completed transfer of responsibility for a message from a gateway, X.400 link, or other MTA into the local MTA.
1	Probe transfer in	The MTA completed transfer of responsibility for a probe from a gateway, X.400 link, or other MTA into the local MTA.
2	Report transfer in	The MTA completed transfer of responsibility for a report from a gateway, X.400 link, or other MTA into the local MTA.
4	Message submission	A message was submitted by a local e-mail client (usually through the Information Store/MDB).
5	Probe submission	An X.400 probe was submitted by a local e-mail client (usually through the Information Store).

6	Probe transfer out	The MTA completed transfer of responsibility for a probe from the local MTA to a gateway, X.400 link, or another MTA.
7	Message transfer out	The MTA completed transfer of responsibility for a message from the local MTA to a gateway, X.400 link, or another MTA.
8	Report transfer out	The MTA completed transfer of responsibility for a report from the local MTA to a gateway, X.400 link, or another MTA.
9	Message delivered	The MTA completed delivery of a message to local recipients (usually through the Information Store).
10	Report delivered	The MTA completed delivery of a receipt or NDR to local recipients (usually through the Information Store).
26	Distribution list expansion	The MTA has expanded a distribution list to produce a new message that has recipients who are distribution list members.
28	Message redirected	The MTA has redirected a message or probe to an alternate recipient because of incorrect configuration data for the original recipient, or failure to route the object or reassignment of data contained in the message.
29	Message rerouted	The MTA has rerouted a message, report, or probe because of problems with next route X.400 link or MTA.
31	Downgrading	The MTA has mapped a message, report, or probe into the 1984 X.400 protocol before transferring it to a remote 1984 MTA.
33	Report absorption	The MTA has scheduled a report for deletion because the user did not request it. In X.400 protocol, NDRs are always routed back to the sending MTA even if the user did not request a report.
34	Report generation	The MTA has created a delivery receipt or NDR.
43	Unroutable report discarded	The MTA has discarded a report because the report cannot be routed to its destination.
50	Gateway deleted message	The administrator deleted an X.400 message that was queued by the MTA for transfer to a gateway. No delivery report is

		generated.
51	Gateway deleted probe	The administrator deleted an X.400 probe that was queued by the MTA for transfer to a gateway. No delivery report is generated.
52	Gateway deleted report	The administrator deleted an X.400 report that was queued by the MTA for transfer to a gateway. No delivery report is generated.
1000	Local delivery	The sender and recipient are on the same server.
1001	Backbone transfer in	Mail was received from another Messaging Application Programming Interface (MAPI) system across a connector or gateway.
1002	Backbone transfer out	Mail was sent to another MAPI system across a connector or gateway.
1003	Gateway transfer out	The message was sent through a gateway.
1004	Gateway transfer in	The message was received from a gateway.
1005	Gateway report transfer in	A delivery receipt or NDR was received from a gateway.
1006	Gateway report transfer out	A delivery receipt or NDR was sent through a gateway.
1007	Gateway report generation	A gateway generated an NDR for a message.
1010	SMTP queued outbound	Outbound mail was queued for delivery by the Internet Mail Service.
1011	SMTP transferred outbound	Outbound mail was transferred to an Internet recipient.
1012	SMTP received inbound	Inbound mail was received by the Internet Mail Service.
1013	SMTP transferred inbound	Mail received by the Internet Mail Service was transferred to the Information Store.
1014	SMTP message rerouted	An Internet message is being rerouted or forwarded to the proper location.
1015	SMTP report transferred in	A delivery receipt or NDR was received by the Internet Mail Service.
1016	SMTP report transferred out	A delivery receipt or NDR was sent to the Internet Mail Service.
1017	SMTP report generated	A delivery receipt or NDR was created.
1018	SMTP report absorbed	The receipt or NDR could not be delivered.
1019	SMTP submit	A new message is submitted to Advanced

	message to AQ	Queuing.
1020	SMTP begin outbound transfer	A message is about to be sent over the wire by SMTP.
1021	SMTP bad mail	The message was transferred to the badmail directory.
1022	SMTP AQ failure	A fatal Advanced Queuing error occurred. Information about the failure is written to the Event Manager.
1023	SMTP local delivery	A message was successfully delivered by a store drive (logged by Advanced Queue).
1024	SMTP submit message to cat	Advanced Queuing submitted a message to the categorizer.
1025	SMTP begin submit message	A new message is submitted to Advanced Queuing.
1026	SMTP AQ failed message	Advanced Queuing could not process the message. The message will be NDRed or put into badmail.
1027	SMTP submit message to SD	A message was submitted to the store driver by the MTA.
1028	SMTP SD local delivery	Store driver successfully delivered a message (logged by store driver).
1029	SMTP SD gateway delivery	Store driver transferred the message to the MTA.
1030	SMTP NDR all	All recipients were NDRed.
1031	SMTP end outbound transfer	The message was successfully transferred outbound.

Event Log Best Practices

- Event logs consume disk space. You must plan for this and monitor so that the event logs do not fill your disks and stop operations. Since the information in the log is essential to capacity planning, detailed troubleshooting, and trend analysis, you should disable circular logging and institute procedures to collect and centrally archive event logs across your organization. You can use the Dump Event Log(dumpel.exe) tool in the Windows 2000 Resource Kit to dump archived event logs to a tab-separated text file.
- Name your event logs so that they are easy to manage in quantity and retrieval; for example, machinename_date_App (myserver_8_1_00_E2K).
- The filtering function for routinely viewing event logs can consume resources on remote systems. Make sure the **Save Settings on Exit** options is turned **OFF** on the monitoring workstations.
- You can conserve network bandwidth when reviewing large event logs on a remote system by using the **Search** function for specific events by **Type**, **Source**, or **Category**.

Perfmon/Sysmon

You can use the Perfmon to configure your alerts and notifications, log entries, script commands and automated corrective actions.

You can use the System Monitor tool, (Sysmon) available by choosing **Performance** from the **Administrative Tools** group, to chart activity in real time or display information contained in a log file. The real-time view is an excellent snapshot view of your system and can give you a quick indication of system health.

Recommended counters to monitor are:

Object	Counter
Process (for the individual Exchange processes)	%Processor Time Working Set
Microsoft SMTP Service	Messages Sent/Second Remote Queue Length Local Queue Length Remote Retry Queue Length Local Retry Queue Length

MSExchangeMTA*	**Work Queue Length** **Messages/Sec**
MSExchangeMTA Connections	Queue Length
MSExchangeIS	User Count
MSExchangeIS Private + Public	Average Time for Delivery Average Time for local Delivery Outgoing Queue Length Incoming Queue Length Active Connections Message Submitted/min Messages Delivered/min Replication Receive Queue Size
Physical Disk (for all drives)	% Disk Read Time % Disk Write Time Current Disk Queue Length
Server	Bytes Total/sec

* This is your best first indicator of potential problems—the “canary in the coal mine” metric.

Note that because of the improved security in Windows 2000, by default your operators will not have permissions to monitor remote systems. The Performance Logs and Alerts service is started under the local computer's system account by default. Normally, the system account only has permission to access services and resources on the local computer, not logs on network computers. The remote system will only allow network connections with user accounts that have the appropriate permissions. To delegate this permission to your operators:

1. Right-click **My Computer**, and then click **Manage**.
2. Open **Services and Applications**.
3. Click **Services**.
4. Right-click **Performance Logs and Alerts**, then click **Properties**.
5. Click the **Log On** tab, and then click **This account**.
6. Enter the user account, and then type a password with sufficient credentials to gain access to the remote computer according to your security and administration model.

Message Tracking Center

Exchange 2000 has a new message tracking log format, but the features

of the Message Tracking Center are much as in the previous version. The tool can be used to track messages end-to-end through the Exchange system.

End to End test (probe)

You can set up test mailboxes on each storage group, and use them to send pre-written test mail messages around your organization to monitor compliance with your SLA metric. These test mailboxes can also be used to quickly troubleshoot a problem and determine if it is localized to that particular storage group.

You can script this procedure with the MAPIsend tool in the Exchange 2000 Resource Kit to proactively monitor service level compliance in a polling model. Set the script to run at the service level metric (for example, every 5 minutes). Log your results for trend analysis and capacity planning, and set your alerts to email you of unacceptable performance.

Once you have established your test mailboxes, you should hide them from the Global Address List (GAL). You can script this procedure using ADSI to proactively hide the entered user from all address Lists. Note that in an ASP environment, this might not be the best practice. You might have multiple Address Lists (for example, for multiple companies hosted on the same server). A sample VB script for doing this is included below:

```
' Binding to the user object using the common name + OU it’s located in + Domain Name’

Dim oUser
Set oUser = GetObject ("LDAP://cn=Testmailbox Name, cn=users, dc=Domain, dc=com”)
' Update the selected attribute for this specific user account’

oUser.msExchHideFromAddressLists = True
oUser.SetInfo
MsgBox "User has been successfully hidden from the GAL.”
```

You can perform this action in reverse simply by changing the Boolean value of:

```
oUser.msExchHideFromAddressLists into FALSE, e.g:
oUser.msExchHideFromAddressLists = False
```

For more info on using ADSI, see the following articles:

http://www.microsoft.com/windows2000/library/howitworks/activedirectory/adsilinks.asp, and http://msdn.microsoft.com/library/psdk/adsi/ds2prggd_ret_0ko9.htm

You can also configure MAPIsend to send performance monitor alerts, backup job status, and disk quota status in addition to test messages. Of course, if that particular server is having problems, MAPIsend will not be able to deliver these messages.

Active Directory Tools

As previously mentioned, a fully functional Windows 2000 Active Directory is an essential pre-requisite for the installation of Exchange 2000 in your environment. Just as your Exchange 5.5 administrators oversaw the Exchange directory performance, you must monitor the health of your Active Directory Exchange information. Depending on the security and administration model you chose, your advanced administrators and/or network support specialists can use a variety of command-line tools to configure, manage, and troubleshoot Active Directory. These support tools are included available on the Windows 2000 Server compact disc in the \SUPPORT\RESKIT folder. Table 5 lists the tools in relative order of importance for monitoring use.

Tool	Description
REPAdmin	Check replication consistency between replication partners, monitor replication status, display replication metadata, force replication events and knowledge consistency checker (KCC) recalculation.
REPLMon	Display replication topology, monitor replication status (including group policies), force replication events and knowledge consistency checker recalculation.
ADSIEdit	A MMC snap-in used to view all objects in the directory (including schema and configuration information), modify objects and set access control lists on objects.
LDP	Allows LDAP operations to be performed against Active Directory. This tool has a graphical user interface.
DNSCMD	Check dynamic registration of DNS resource records, including Secure DNS update, as well as deregistration of resource records.
DSACLS	View or modify the access control lists of directory objects.
NETDIAG	Check end-to-end network and distributed services functions.
NLTest	Check that the locator and secure channel are functioning.
DSAStat	Compare directory information on domain controllers and detect differences.
SDCheck	Check access control list propagation and replication for specified objects in the directory. This tool enables an administrator to determine if access control lists are being inherited correctly and if access control list changes are being replicated from one domain controller to another.
ACLDiag	Determine whether a user has been granted or denied access to a directory object. It can also be used to reset access control lists to their default state.
DFSCheck	Command-line utility for managing all aspects of Distributed File System (Dfs), checking the configuration concurrency of Dfs

	servers, and displaying the Dfs topology.

For detailed information on using the support tools to monitor and troubleshoot your Active Directory, type “command reference” at either the **Index** or **Search** tab in Windows 2000 Online Help.

To determine that an incident is related to Active Directory and not Exchange 2000, start by checking directory replication status using Replmon.

The minimum permission necessary is "Manage Replication Topology" for "This object only" on the appropriate directory partition. For the domain directory partition, you can grant this permission through the Active Directory Users and Computers snap-in, or you can use Adsiedit.msc, an administrative tool included in the Support tools for Windows 2000.

To delegate the permission to monitor the schema and configuration directory partitions using Adsiedit:

1. Log on to the domain controller as an Administrator of the root domain of the forest.
2. Install the Windows 2000 Support tools if they are not already installed. You can do this through **Control Panel\AddRemove Programs**.
3. Run Setup.exe from the Support\Tools folder of the Windows 2000 Server or Windows 2000 Professional CD-ROM.
4. Run Adsiedit.msc and expand the **Configuration Container** or **Schema** node, whichever is appropriate.
5. Each node contains a child object that begins with "CN=". Right-click this object, and then click **Properties**.
6. On the Security tab, click **Add**.
7. Double-click the user or group to which you want to delegate permissions, and then click **OK**.
8. With the user or group highlighted, click the check box in the **Allow** column for the following permission: **Manage Replication Topology**
9. Click **OK**.

To delegate the permission to monitor domain directory partition status:

1. Open the Active Directory Users and Computers snap-in as an administrator of the domain.
2. On the **View** menu, click **Advanced Features** so there is a check mark next to it.

3. Right-click the root domain object, and then click **Properties**.
4. On the **Security** tab, click **Add**.
5. Select the user or group to which you want to delegate the permissions, and then click **OK**.
6. With the user or group still highlighted, click the check box in the **Allow** column for the following permission: **Manage Replication Topology**
7. Click **OK**.

Perfmon counters to monitor

Object	Purpose
NTDS	Monitor whether the server is receiving timely updates
NTDS:DRA Pending Replication Synchronizations	Monitors the number of directory synchronizations that are pending but not yet processed. This tells you if the server has a replication backlog.
NTDS:DRA Inbound Full Sync Objects Remaining	The number of objects remaining until the full synchronization process is completed.
NTDS:DRA Inbound Object Updates Remaining in Packet	The number of objects received in the current directory replication update packet that have not yet been applied to the local server. This tells you whether the monitored server is receiving changes, but is taking a long time to apply them.
NTDS:DRA Outbound Properties/sec	The number of properties sent per second. This tells you whether a source server is returning objects or not.
NTDS:DS Threads in Use	The current number of threads in use by the directory service (different from the number of threads in the directory service process). A consistently high number might indicate a bottleneck and the need for additional processors.

Event Log entries to monitor

The Windows NT 4.0 Event Viewer (and earlier versions) ignores any logs other than the Application, Security, and System logs; however, the Windows 2000 Event Viewer includes three new event logs:

- Directory Service event log
- DNS Server event log
- File Replication Service event log

The Directory Service and File Replication Service event logs are exposed in Event Viewer on Windows 2000 domain controllers only. The DNS Server event log is available on DNS servers only. Windows 2000 Event Viewer automatically recognizes any active event logs on a computer.

To view these event logs over the network:

1. Click the **Event Viewer** (Local) folder.
2. On the **Action** menu, click **Connect to another computer**.
3. Click the computer name for the domain controller or DNS server to expose their event logs.

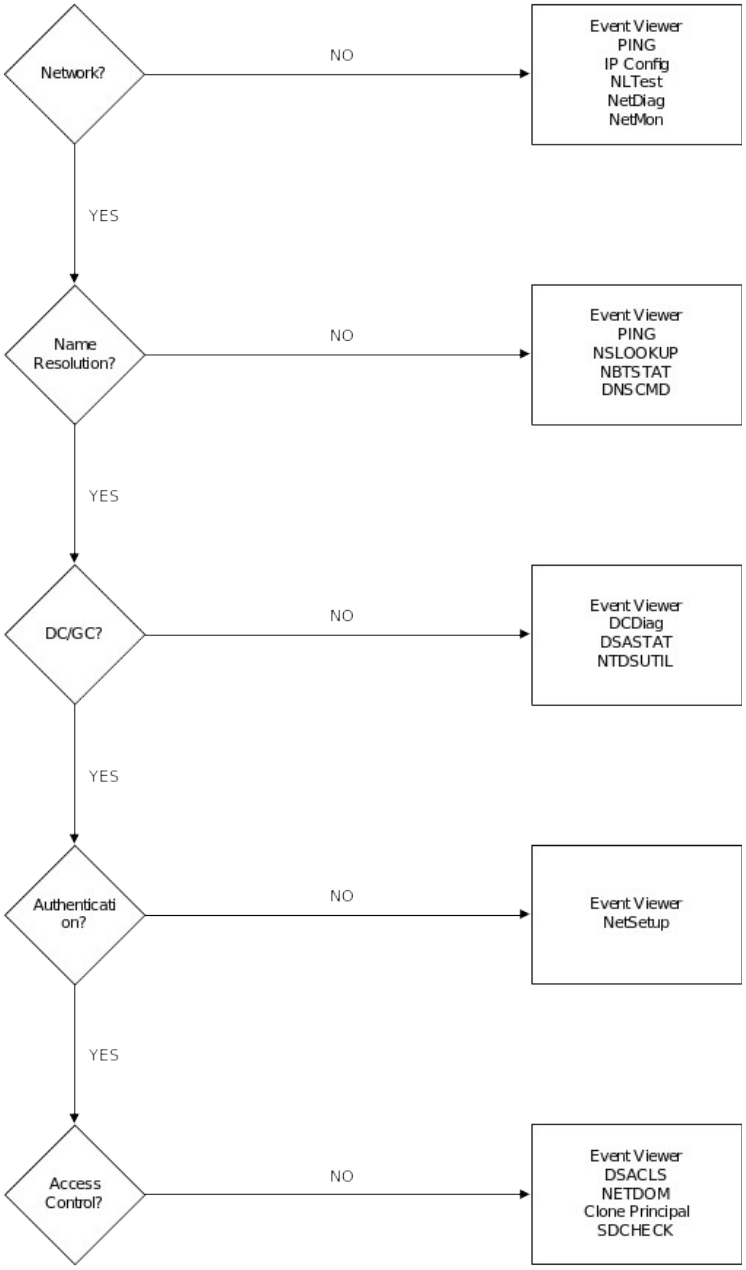
If the domain controller or DNS server event logs are not available using this method, follow these steps:

4. Save the event logs by clicking the event log you want, and then clicking **Save Log File As** on the **Action** menu.
5. Load the logs onto another computer by clicking **Open Log File** and then clicking the file that you saved. This action requires that you specify a log file type. You can select any of the existing log types, but the event categories and descriptions are either not found or are incorrect.

Object	Purpose
NTDS KCC Event ID: 1311	Indicates a site has been orphaned from the replication topology.

Troubleshooting checklist

1. Are directory clients timing out, or are their connections being refused by the server?
2. Are all network components (routers, hubs, switches, cables) between the client and the server operational?
3. Is the DC or GC operational? If not, can you determine whether this is a hardware or software problem?
4. Is the directory server process running? If so, is it consuming higher-than normal CPU cycles, or causing excessive disk activity?
5. If the directory server process is not running, did it fail when processing a specific or particular type of client request? Does it fail each time it receives/processes such a request? If so, it may indicate a denial-of-service attack.


Network?
NO
Event Viewer
PING
IP Config
NLTest
NetDiag
NetMon
YES
Name Resolution?
NO
Event Viewer
PING
NSLOOKUP
NBTSTAT
DNSCMD
YES
DC/GC?
NO
Event Viewer
DCDiag
DSASTAT
NTDSUTIL
YES
Authenticati on?
NO
Event Viewer
NetSetup
YES
Access Control?
NO
Event Viewer
DSACLS
NETDOM
Clone Principal
SDCHECK

Related Topics

“Active Directory Diagnostics, Troubleshooting, and Recovery” gives excellent advice on troubleshooting:

http://www.microsoft.com/TechNet/win2000/win2ksrv/reskit/dsgch10.asp

“Windows 2000 – Deletion of Critical Objects in the Active Directory” http://support.microsoft.com/support/win2000/ad.asp

“MS Exchange 2000 Server Directory Access and Integration with MS Windows 2000”

http://www.microsoft.com/TechNet/exchange/technote/wininteg.asp

See also Q259302 How to Optimize Active Directory Replication in a Large Network

See also Q259302 Windows 2000 DNS Event Messages 1 Through 1614

Exchange Monitoring and Status Tool

The Exchange Monitoring and Status Tool is located under **Tools** in the Exchange System Manger MMC snap-in. It replaces the Server Monitor and Link Monitor tools you used Exchange 5.5, and allows you to configure alerts on continued growth of queues rather than a static threshold.

All servers and connectors in the organization are listed in the **Status** container with a filtering option to limit which are displayed. Each connector is automatically monitored and displays as available or unavailable. For each server, one or more resources can be monitored. By default, a resource called **Default Exchange Services** is monitored which includes the following group of services:

- Microsoft Exchange Information Store
  - MSExchangeIS, Active Connection Count. - This measures the number of logons to the Store Service. This number should be greater than zero. If the server has active mailboxes and there are zero connections then a problem exists. Use a test account to see if there is a problem making a connection to the server.
- Microsoft Exchange MTA Stacks
  - MSExchangeMTA, Work Queue length
  - MSExchangeMTA, Messages Delivered per Minute
- Microsoft Exchange Routing Engine
- Microsoft Exchange System Attendant
- Simple Mail Transport Protocol (SMTP)
- World Wide Web Publishing Service

Other services can be added to the Default Exchange Services resource or to the separate Windows 2000 service resource. A complete list of

resources that can be monitored is listed below:

Resource	Purpose
Default Exchange Services	Monitors specified services. Can optionally change to warning or critical state if a service is not running.
Available Virtual Memory	Monitors available virtual memory with control over the thresholds for warning or critical state and how long the threshold must be exceeded to change the state.
CPU Utilization	Monitors available CPU utilization with control over the thresholds for warning or critical state, and how long the threshold must be exceeded to change the state.
Free disk space	Monitors available disk space on a specified drive with warning and critical thresholds.
SMTP queue growth	Monitors growth in SMTP queues with thresholds in minutes for warning or critical state when queues grow continually.
Windows 2000 service	Monitors specified services. Can optionally change to warning or critical state is a service is not running.
X.400 queue growth	Monitors growth in X.400 queues with thresholds in minutes for warning or critical state when queues grow continually.

When any of the monitored resources for a server change state, the monitor will display a warning or critical state. You can create email, page or script notification entries in the notifications container to trigger when status changes on servers or connectors. Available parameters for configuring notifications are:

Parameter	Choices
Monitoring server	The server that performs the monitoring
Servers and connectors to monitor	This server, all servers or connector, any server or connector in the routing group or a customized list of servers or connectors.
Notify when monitored items are in	Controls whether notification triggers on status change to warning or critical.

When a notification triggers, you can configure three options for action:

- E-mail – Recipients, sending server, subject line, and message body

- Page – Pager number and touch-tone message to send
- Script – Path to executable and command line switches to use

You can use this tool to establish comprehensive monitoring of all Exchange 2000 servers and connectors. Set your triggers to appropriate levels based on your baseline performance analysis to avoid flooding the logs.

Queue Viewer

You can use the new Queue Manager in the Exchange System Manager (ESM) to monitor the state of all queues. If you notice a problem in the MTA stack monitor, use the Queue Viewer to freeze a message in the queue, return it to the sender, or delete it.

Resource Requirements

This section directs you to the resources you will need to monitor and maintain your Windows 2000 Active Directory and Exchange 2000. The exact number of resources you will need will depend on the architecture you designed, the number of servers to monitor, the security and administrative structures you implemented, the skill level of your resources, and the capabilities and limitations of any third-party tools you will be integrating into your processes.

Teaming

Deployment of Exchange 2000 is a cooperative effort between your messaging, infrastructure engineering, network administration, and directory services teams. Tight coordination between these teams is critical to your Exchange 2000 operations.

Tasks assignment:

Task	Frequency (minimum)	Responsible Party
Perform backups	Daily	Operations
Perform recovery drills	Weekly	Service Management/Operations
Monitor Exchange Servers	Daily	Operations
Review Event Logs	2/weekly	Service Management/Operations
Monitor Network/Hardware/Windows 2000 server specific	Daily	Operations

objects		
Review/Update configuration	Ongoing	Service Management Change Management

As an example, the LMO Exchange 2000 deployment high-level tasks were:

- Deploy Exchange 2000 worldwide with a 5 minute message delivery SLA for 80% of all mail worldwide
- Migrate more than 56,000 mailboxes, each with a 100 MB mailbox limit
- Upgrade more than 125 servers, 72 sites worldwide
- Accommodate a message database backup restoration time of less than one hour

The example LMO deployment team consists of the following resources:

Function/Role	Full Time Equivalent (FTE)
Program Management	5 (deploy Core Messaging, Wireless, Instant Messaging, Exchange Conferencing Service, Outlook Web Access, Unified Messaging)
Operations	24 (24X7X365 worldwide)
Service Management	4
Engineering	4 (consolidate servers in Corporate headquarters, consolidated 24 mailbox servers of 1,000 users (average) each to 8 servers with an average 4,000 users each)
Support	3
Directory Management	2 (manages Active Directory Connector connection agreements during migration, and troubleshoots directory issues)
Network Management	1

After successful deployment, because they use several third party tools for centralized SNMP monitoring and event log trigger e-mail, the example LMO found they require roughly 1 FTE per 60 servers to maintain their Exchange organization. Without centralized monitoring and alerting they require 1 FTE per 25 servers.

Security and Account Privileges

To execute most monitoring tasks, you will need the following minimum Windows 2000 account privileges:

- View Only Exchange Administrator

For troubleshooting you may also need the following privileges:

- Schema Administrator
- Domain Administrator
    - Enterprise Administrator
- Windows NT 4.0 Domain Administrator
- Exchange 5.5 Administrator
- Exchange Full Administrator
- Knowledge of the Exchange 5.5 Service Account name and password.

The security and administration model you determined in the first part of this chapter will guide you in assigning the appropriate permissions structure to your monitoring resources and escalation model.

Escalation Model (example)
To meet your defined service level agreement metrics, you need to plan for responses to problems identified by routine monitoring. A good way to plan this process is to define an escalation model that details roles, responsibilities, and clear escalation paths and times. An example escalation model is provided below.

Escalation Model Objective
Define the components and associated processing times for incident escalation within a three tiered support model to insure that the stated Mean Time To Repair/Resolve (MTTR) goals are met for each incident severity during the course of a fiscal month.

This model shows three tiers of support for Exchange 2000 problems identified during regular monitoring. For the majority of incidents, users deal with the first tier only.

Incident Escalation Processing Components and Definitions
Sample Incident severities:

1-Immediate: An unscheduled site or service outage that adversely impacts the user reducing access or functionality by 50% or more; or, the outage is impacting 50 or more users.

2-High: An unscheduled site or service outage that adversely impacts the user, reducing site/service access or functionality by less than 50%, and is significantly impacting normal business operations.

3-Normal: An unscheduled site or service outage that represents a minimal reduction in user access or functionality, or impacts 0 to 10 users.

4-Low: A task and/or preventative maintenance that can be completed as time permits since user impact may not exist. This is also used to list events, tasks, and data for tracking and status purposes only. This includes alerts indicating the status and outcome of automated scripts, alerts on network capacity trends, upcoming maintenance periods, and so on.

Incident severity assessment and ticket generation: the amount of time that a support tier has to review the incident, determine its severity, and create a trouble ticket. Note: not all levels of the tiered support model generate trouble tickets.

Incident trouble shooting: a guideline for the maximum amount of time that a support tier should work on a trouble ticket without being able to determine what the resolution path should be. Trouble tickets that

exceed this value should be escalated to the next support tier once the accompanying escalation documentation has been completed. Once the incident's resolution path has been determined, the time required to completely resolve the incident is not included in this time period.

For example if a first tier's trouble shooting guideline is 30 minutes, it might take 20 minutes to determine that a DC/GC problem is preventing mail delivery. Since a resolution path was determined within the 30 minute guideline, the incident is not escalated to the next tier. While the time associated to determine and resolve the DC/GC issue might exceed the stated 30 minute trouble shooting guideline, it is not taken into consideration since the focus is on resolution path determination time and not total resolution time.

Note that the stated troubleshooting times should be used only as a guideline. They should not be considered a hard-stop time-based deadline that requires an escalation regardless of the troubleshooting progress achieved. This is a model to get you started: adapt it to your organization's circumstances.

Incident Escalation Handoff: The trouble ticket is transferred to the next support tier's queue either from within the ticket tracking application and/or by sending the incident details in a pre-prescribed format for the next support tier to process.

The specific documentation/forms to include in an incident escalation should be agreed upon by the interacting support tiers in advance.

First Tier – Process

1. Log the problem in a shared problem-tracking application from which a daily report is generated.
2. Give 30 minutes best effort to solve problem.
3. Log the problem on the form and escalate as follows:
   - Direct contact with the people from second tier support.
   - If nobody is available, escalate using a radio.
   - If there is no response to the radio message, page the second level person on call.
   - If the person on call does not respond in 15 minutes, page a group manager.
   - If the group manager does not respond in 15 minutes, directly page their boss.
4. Put an entry into the daily log with time of escalation and relevant details.

Second Tier – Solution

This tier is responsible for providing a solution, or escalating to the third tier. If the problem appears to be beyond the second tier capacity within

the guidelines, then the third tier is contacted according to the following process:

5. Give best effort for 30 minutes.
6. Update the already open form in the problem tracking application
7. Keep the person from first level support who reported the problem in the loop, and update them (over the phone or in person) before the next escalation
8. Before escalation, make a copy the form.
9. Escalate through a pager as follows:
   - Page the third tier support person on call, and give them the original incident report form
   - If there is no response in 15 minutes, page the second and third level support managers
   - If there is no response in 15 minutes, page their respective managers
10. Put an entry into the daily log with time of escalation and relevant details.

Third Tier – Crises Management

The crisis management group is ultimately responsible for providing a solution or researching the issue so it can be resolved.

IT Management

IT management should be notified through a daily report listing:

- Severity 1 incidents that exceed two times the designated mean time to resolve.
- Significant regional outages escalated to tier 3.

Operating System Availability

There are several variations of availability, including planned availability and total availability. Total availability is defined as the percentage of up time over total run time, and can be computed easily using the information in the System Event Log.

System recoverability is measured as the length of time a system is unavailable following a system outage. Typically, this is reported as mean time to repair. It is easy to measure mean time to repair using the Windows 2000 operating system Event Log. An outage begins when a system is shut down and ends when the system is restarted.

Perfmon System Uptime Counter

SUMMARY

The System Uptime counter measures the time, in seconds, that the system has been up. PerfMon graphs the results on the screen as they are gathered, and allows you to export the results to Excel or other applications for reporting purposes.

Recommended counters to monitor are:

Object	Purpose
Source: Event Log Service Event ID: 6005	Startup Event: Time the operating system becomes available to Exchange.
Source: Event Log Service Event ID: 6006	Clean Shutdown Event: Time the system became unavailable to Exchange (shutdown by the user or WIN32 API).
Source: Event Log Service Event ID: 6008	Dirty Shutdown Event: Recorded when the system restarts from a “dirty” shutdown, plus or minus 5 minutes (default registry setting for TimeStampInterval for “last alive” timestamp).

Information is power. To efficiently deliver your messaging and collaboration service levels you will need both daily and long term information. You must have a detailed understanding of your Exchange (5.5 and 2000) architecture to analyze and understand the value of the information you collect. Finally, performance is related to usage. Any given value you monitor must be evaluated against both usage and architecture.

In this chapter, you examined the close link between your Exchange 2000 architecture, server configurations, service level metrics, and operational team structure. Most of these will probably remain substantially the same during your migration or coexistence period, while you still have Exchange 5.5 servers in your environment. The biggest differences are the new dependencies associated with Exchange 2000 and Active Directory, the administrative and security model consolidations you may have made to reduce operating costs, and, when your environment is pure Exchange 2000, SMTP monitoring.

Links

WMI scripting. This paper presents an overview of the Windows Management Instrumentation (WMI) Scripting API. The Windows Management Instrumentation is an implementation of the Distributed Management Task Force’s (DMTF) Web-Based Enterprise Management (WBEM) initiative, which provides standards for accessing and sharing management information in an enterprise environment.

http://www.microsoft.com/windows2000/library/howitworks/management/wmiscripts.asp

Building Management Components for Microsoft Exchange 2000 Server. This article discusses building system management software for Microsoft Exchange 2000 Server.

http://msdn.microsoft.com/library/techart/e2k_cmpts.htm